## REMARKS

This responds to the Office Action mailed on March 10, 2005, and the references cited therewith and the Advisory Action mailed June 3, 2005.

Claims 1 and 3 are amended, no claims are canceled, and no claims are added; as a result, claims 1-15 remain pending in this application.

### *§103 Rejection of the Claims*

Claims 1-15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Shear et al. (U.S. 6,157,721) in view of Santon et al. (U.S. 5,058,162). Applicant traverses this rejection based on the remarks set out below.

Claim 1

Claim 1 has been amended by specifying that the attribute data comprises information to find in the protected contents information on the appropriate protocol for **establishing a communication interface**. This amendment finds basis in the application as filed on page 6, lines 8-9 and page 7, lines 5-7.

Claim 3

Claim 3 has been amended on the basis of the same passages as mentioned above with regard to claim 1.

It is submitted that the subject-matter of claims 1 and 3 is not obvious with regard to the cited references. In particular, the feature of information to ***find*** in the protected contents information on a protocol is not disclosed as being part of any of the systems of the cited references. Furthermore, none of the items of cited references discloses protected contents

comprising information on the appropriate protocol for **establishing a communication interface** between a secure device and a content player.

US 6,157,721 (hereinafter: D1) discloses two systems, inasmuch as it also discloses in brief a system described in U.S. patent application 08/388,107 ("the Ginter et al. specification").

In the passage on column 3, lines 16-35, it is disclosed that Ginter *et al.* describes a protected processing environment that can execute computer code which the Ginter *et al.* disclosure refers to as "load modules" (column 3, lines 21-23). Load modules may contain algorithms, data, cryptographic keys, shared secrets and/or other information that permits a load module to interact with other system components (e.g. other load modules, and/or computer programs operating in the same or different protected processing environment) (column 3, lines 28-32). Insofar as the contents of US patent application 08/388,107 have been made publicly available, there is no disclosure of providing a protected contents containing the encrypted data, the secure device data, protocol information and attribute data on the different parts inside the protected contents. In particular, **there is no disclosure of information to find in the protected contents information on the appropriate protocol**. This is true regardless of whether one considers cryptographic keys, shared secrets and/or other information that permits interaction between two computer code modules to equate to information on a protocol for communication between the content player and a secure device.

D1 also fails to disclose information to find in protected contents protocol information as recited in claims 1 and 3. Instead, D1 discloses an assurance level II electronic appliance, an example of which might be a general purpose personal computer equipped with a hardware integrated circuit secure processing unit that performs some secure processing outside of the SPU (column 16, liens 52-60). There is no disclosure of information in the load module 54 being

**used to establish an interface** between the general-purpose personal computer and SPU. Consequently, there is no information to find in the load module 54 information on the appropriate protocol.

D2 (US 5,058,162) similarly doesn't disclose information to ***find*** in protected contents information on a protocol for establishing an interface between a content player and a secure device. Instead, D2 describes a region access map which logically divides the user data file area of the disk into a series of contiguous physical regions for the purpose of identifying where *data files* ... are located (column 6, lines 44-48). D2 discloses a disk drive provided with conventional drive controller hardware and drive controller firmware (column 7, lines 32-35). The drive is operably attached to a conventional minicomputer or microcomputer (column 7, lines 60-64). A security software program 128 is comprised in drive controller firmware 114 (column 7, lines 46-49). Thus, there is no disclosure of any information on the disk 10 for establishing **an interface between a secure device and a content player**, let alone of information for finding such protocol information on the disk 10. Instead, the security software program is initiated by other drive controller firmware *in response to* the drive's reading of the security disk header of the disk 10. (column 8, lines 28-30).

In short, because D1 and D2 each fail to disclose information to ***find*** in protected contents information on a protocol for communication between a content player and secure device, the cited references do not teach all the limitations of claims 1 and 3, so that the case against those claims on grounds of obviousness is incomplete.

An example effect provided by the feature of attribute data comprising information to find in the protected contents information on the appropriate protocol for communication between the content player and the secure device, is to **allow creation of a flexible interface**

between a content player and a secure device in an efficient and secure manner. Because information for establishing the interface is provided in the protected contents, a flexible interface can be established. Because the information is provided in the same protected contents as the encrypted data and secure device data, the methods according to the invention are efficient. Due to the presence of attribute data including information to find in the protected contents information on the appropriate protocol for establishing the communication interface, the entire protected contents need not be accessible to the content player. This makes the methods relatively secure.

D1 and D2 fail to disclose methods providing the same effects. In particular, in D1, the interface between the Secure Processing Unit and general-purpose personal computer is fixed, thus relatively inflexible. In D2, the interface between the decryption chip 120 and drive controller hardware 112 is fixed. It follows that the present invention provides effects not previously attainable using the teachings of the cited references. This underscores the inventive character of the present invention.

## CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at 408-278-4041 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

WILHELMUS GERARDUS PETRUS MOOIJ

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
408-278-4042

Date 7/19/2005

By Mark R. Vatuone
Mark R. Vatuone
Reg. No. 53,719

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop RCE, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 19 day of July, 2005.

Dawn R. Shaw
Name

Dawn R Shaw
Signature